DIRECCION DE ESTRUCTURAS ADMINISTRATIVAS

Y

SISTEMAS DE INFORMACIÓN

DEPARTAMENTO DE SISTEMAS DE INFORMACION

NORMAS BASICAS DE

AUDITORIA DE SISTEMAS

INDICE

INTRODUCCIÓN

Objetivos

Control Interno

Normas Básicas de Auditoría de Sistemas

CRITERIOS DE EVALUACION

- De la organización del área de sistemas de información
- Documentación exigible
- Seguridad lógica
- Sistemas aplicativos y Registro de movimientos
- Teleprocesamiento y Telecomunicaciones. Redes y accesos remotos
- Seguridad física
- Política de backups
- Derechos del usuario

CONCLUSIONES

APENDICE

Fuentes bibliográficas - Direcciones en la Web

INTRODUCCIÓN

Objetivos

El objetivo de esta obra es definir los criterios de auditoría de sistemas a utilizar en nuestro trabajo específico sobre el Gobierno de la Ciudad de Buenos Aires (G.C.B.A). Planteamos, como primer paso, utilizar criterios básicos y generar normas que permitan alcanzar un estado inicial de seguridad y auditabilidad en los sistemas de información y las tecnologías asociadas.

El objeto a auditar, los sistemas de información y las tecnologías de la información en el G.C.B.A., es tan amplio y heterogéneo que invalida el uso de recetas y/o soluciones rígidas. En consecuencia, estas normas deberán aplicarse teniendo en cuenta las particularidades y las características de cada área, el valor de la información y la finalidad de la misma.

Se intenta establecer criterios de auditoria exigibles y alcanzables. Entendiendo que, si bien constituyen una herramienta para el auditor de sistemas, también son muy importantes para el auditado ya que le permiten conocer por anticipado las reglas con las que será examinado. Por otra parte manejar lineamientos más o menos homogéneos con otros organismos de control, en la medida que esto no comprometa nuestra independencia, homogeneizará y simplificará la tarea de los auditados ahorrando esfuerzos. Consideramos que esta tarea debe realizarse entre todos los funcionarios y agentes comprometidos en el manejo de la información, y no sólo con aquellos que están a cargo de las áreas informáticas.

Esta TRINIDAD está compuesta por 3 partes. Una vez aprobadas estas normas y en base a las mismas definiremos la metodología en forma de una Guía de Auditoría que usaremos como herramienta de campo en la A.G.C.B.A., con sus pasos, productos e informes. La tercera parte está constituida específicamente por los listados de control.

Presupuestos básicos

La información es un activo y el GCBA debe considerarla como tal. También es un componente indispensable de la gestión de gobierno. El crecimiento de los procesos automatizados para el manejo de la información aumentan la importancia y la necesidad de preservarla con los deberes y el cuidado propios de un activo relevante.

Control Interno.

El entorno de control interno en un organismo está dado, según las Normas Básicas de Auditoría Externa de la AGCBA, por los procedimientos que ayudan a :

- La eficacia y eficiencia de las operaciones

- La confiabilidad de los datos
- La salvaguardia de los activos
- El cumplimiento de las normas

El auditor deberá observar el ambiente de control en los organismos, y aplicar los criterios dentro de la Administración de un modo integral. Estos controles internos deben comprender a todos los elementos que intervienen en el procesamiento de la información (recursos, sistemas, procesos, estructura, cultura de trabajo, tareas y datos).

Debe observar también que las medidas de control existan en todos los niveles de la estructura, mediante la combinación de mecanismos tales como aprobación, autorización, verificación y segregación de funciones.

Los criterios más generales de control interno, orientados a la confiabilidad de los datos y que deben verificarse en el flujo interno de la información dentro de un organismo son:

- Independencia del área de sistemas en la estructura del organismo.
- Independencia del responsable de seguridad de los sistemas de información con relación al área de sistemas.
- Controles por oposición en las tareas.
- Separación lógica de ambientes entre áreas de carga, control y modificación.
- Separación física de operaciones y desarrollo.
- Registro automatizado de las modificaciones realizadas en el sistema (logs).

El auditor debe evaluar el grado en que el no cumplimiento de estas normas básicas aumenta la vulnerabilidad de la información ante los riesgos de amenazas potenciales, imprevistos, accidentes, daños o cualquier acto o evento con efectos adversos.

Se denominan amenazas a los riesgos que afectan a los sistemas, la información y los procesos. La no existencia de mecanismos de control interno aumenta fuertemente la posibilidad de que se concreten amenazas.

Algunos riesgos son:

- **Acceso no permitido**, puede darse por falta de confidencialidad en la clave de uso y/o por uso indebido de puestos de trabajo, uso indebido de recursos o modificaciones no autorizadas

- **Pérdida o destrucción de información,** por falta de resguardo físico y política de backups

- **Fraude**, entendido como la alteración o eliminación de información con carácter doloso

- **Falsificación**, cambiar datos originales

- **Ataques externos y/o internos**

- **Robo de la información**, para su venta o divulgación

Con las comunicaciones se agregan otros riesgos como la negación de servicio y más peligroso, el uso de las propias instalaciones como plataforma de ataque o enmascaramiento de penetración o ataque hacia otra red. En este contexto el control de los virus, macros, gusanos y troyanos debe ser considerado como una práctica obligatoria y permanente.

Normas Básicas de Auditoría de Sistemas de Información

Reproducimos aquí el párrafo de las Normas Básicas de Auditoría Externa de la Auditoría General de la Ciudad (**http://www.agcba.gov.ar**) aprobadas en octubre de 2000 que dice:

"CONCEPTO DE AUDITORIA EXTERNA"

La auditoría externa es un examen global, total e integrado, que tiende al control de la gestión pública desde una perspectiva externa a su propio proceso y que, a diferencia de los otros tipos de control de gestión, está orientada fundamentalmente a promover la mejora de las operaciones de gobierno - en términos de economía, eficacia y eficiencia - y a fortalecer la capacidad sistémica del estado de rendir cuentas de su gestión a la sociedad."

La Constitución de la Ciudad de Buenos Aires establece un sistema integral de control. También la propia Constitución la ley 70 y la ley 325 hablan de aspectos económicos, financieros, patrimoniales, de gestión, de sistemas de información y legalidad.

"Auditoría de Sistemas Informáticos "

Es el examen que consiste en realizar los procedimientos de verificación del correcto funcionamiento de los procesos sistemas de información. Se seleccionan distintos procedimientos de auditoría para controlar la forma en que funcionan las aplicaciones informáticas. Se trata de un examen que se torna imprescindible dado la significativa participación que tiene la informática en la organización de una entidad. "

“CRITERIOS DE AUDITORIA”

A los fines de las presentes normas, se definen los siguientes criterios de auditoria:

a) **Economía**: Se refiere a la adquisición de la cantidad y calidad apropiada de recursos financieros como humanos, materiales, informáticos, tecnológicos, etc. con oportunidad y al más bajo costo y al grado en que los servicios y bienes producidos satisfacen las necesidades para las cuales fueron dirigidos.

b) **Eficacia**: Corresponde al logro de las metas previstas en planes, programas, proyectos, operaciones y actividades, así como la adecuación de los mismos a los objetivos del organismo auditado.

c) **Eficiencia**: Se refiere al uso productivo de los recursos tendiendo a maximizar el producto por recurso utilizado o minimizar los recursos empleados por cantidad y calidad de producto obtenido.

”En los programas de auditoría deberán considerarse los criterios de ética pública, equidad y el impacto ambiental que pudiera configurarse.”

A los conceptos anteriores del las Normas Básicas de Auditoría de la AGCBA sugerimos incorporar las siguientes precisiones:

AUDITORIA DE SISTEMAS.

Conjunto de procedimientos que deben llevarse a cabo para verificar el cumplimiento de los criterios de auditoría correspondientes a los procesos de sistemas de información y las tecnologías asociadas a ellas. Deben estar diseñados guardando relación con el logro de los objetivos de la organización y los recursos aplicados para este fin.

CRITERIOS: En los sistemas de información deben observarse que se cumplan los siguientes criterios esenciales

-Confidencialidad: Condición de salvaguarda de la información a fin de evitar su disponibilidad para personas y/o procesos no autorizados.

-Integridad: Condición en que la información es creada, modificada o eliminada solo por el personal y en las condiciones fijadas por la organización.

-Disponibilidad: Condición en que la información esta en el lugar momento y forma en que es requerido por el usuario autorizado.

-Cumplimiento: Debe darse al cumplimiento a las normas internas y a todas las leyes y reglamentaciones a las que están sujetas las organizaciones públicas.

-Confiabilidad: Los sistemas deben brindar información correcta para ser utilizada en la operatoria de la organización y en la presentación de informes contables y financieros a los usuarios internos , a la Auditoría General del G.C.B.A. y demás organismos de control.

-**Autenticidad**: determinación de quien esta autorizado y quien es el responsable de las autorizaciones.

-Transparencia: La resultante de la aplicación de estos criterios en el manejo de la información lleva a la trasparencia de la gestión, al mejor cumplimiento de los fines de gobierno y a preservar los derechos de los ciudadanos.

Corrientes más modernas de la auditoría de sistemas de información y tecnologías asociadas incluyen cómo criterio la ergonomía y la ecología del entorno en que se desarrollan tareas informáticas intensivas y centros de cómputos. Estos conceptos fueron incluidos en nuestras normas generales al mencionarse el impacto ambiental.

CRITERIOS BASICOS DE EVALUACIÓN

DE LA ORGANIZACION DEL ÁREA DE SISTEMAS DE INFORMACIÓN.

El auditor debe identificar en que lugar dentro de la estructura organizacional está ubicada el área de Sistemas de Información la que deberá depender funcionalmente de un nivel tal que permita garantizar su independencia tanto de las áreas usuarias como de Administración. Concretamente se debe verificar que ningún área de usuarios tenga autoridad para modificar los datos sin pasar por los responsables de sistemas.

Debe observar si existe un plan de Sistemas formal contenga un cronograma de las actividades del área, asignación de prioridades, recursos, sectores involucrados y la totalidad de las tareas a llevarse a cabo durante un período mínimo de 1 año, que permita una supervisión continua y directa de las tareas que realizan los distintos sectores.

Se debe constatar que el área presenta una clara delimitación de las tareas entre desarrollo (si lo hubiera) y mantenimiento de sistemas, Administración de Bases de Datos, operaciones, carga de datos, soporte técnico y supervisión, de manera que se garantice una adecuada segregación de funciones y fomente un control por oposición de intereses.

Asimismo debe verificar si existen políticas generales para el área con una clara definición de las misiones y funciones de todos los puestos de trabajo (responsabilidad, dependencia, funciones que supervisa. etc.), estándares y procedimientos escritos que sean la base de la planificación, el control y la evaluación gerencial.

DOCUMENTACIÓN EXIGIBLE

Debe solicitar la documentación detallada sobre el equipamiento informático, que incluya diagramas y distribución física de las instalaciones , inventario de 'hardware" y 'software" completos, diagramas topológicos y lógicos de las redes, flujo de la información por la red, tipos de vínculos y ubicación de nodos.

El auditor debe observar si existen manuales con estándares de metodología para el diseño, desarrollo y mantenimiento de los sistemas aplicativos. Su aplicación debe regir para todos los nuevos sistemas que se desarrollen y para las modificaciones.

Debe solicitar y controlar la documentación de: los sistemas aplicativos, la operación de los procesos informáticos, los procesos de recuperación de datos y archivos, los procesos de copias y resguardo de datos, la administración de la red de telecomunicaciones, los procedimientos para la puesta en marcha de programas en producción, el tratamiento de los requerimientos de usuarios, los manuales de usuario y los procedimientos de transferencias de información y toda otra tarea significativa de la Dirección o Gerencia.

Esta información comprende tanto al centro de procesamiento de datos principal como a los secundarios, las redes departamentales y al centro alternativo para contingencias.

SEGURIDAD LOGICA

Dentro de la estructura de la organización deberá comprobar si existe una función para la administración y control de la seguridad de acceso a los datos, un responsable de seguridad que sea independiente del área de Sistemas de Información y que se reporte al máximo nivel de autoridad.

Debe observar si existe una política formal de seguridad informática, en la que se detallen como mínimo los siguientes aspectos: nivel de confidencialidad de los datos, procedimiento de otorgamiento de claves de usuarios para el ingreso a los sistemas, y estándares fijados para el acceso de usuarios.

El auditor debe determinar si las claves son personales y secretas. Debe verificar la existencia de un procedimiento de inhabilitación automática de claves de usuarios que no hagan uso de la misma por un período predeterminado y si existe un procedimiento formal para la baja de usuarios que dejen de pertenecer al sector o repartición.

El auditor controlará que el sistema de seguridad mantenga los archivos de claves o "passwords" encriptadas , generar reportes de auditoría sobre intentos de violaciones, el uso de utilitarios sensitivos y las actividades de los usuarios con atributos de administración y accesos especiales, los que deberán mantenerse en archivo durante el tiempo que fijan las normas para cada caso, utilizando para ello soportes de almacenamiento (papel, CD, disco óptico u otras tecnologías de esa características).

Debe verificar la existencia de una adecuada planificación y documentación escrita y actualizada de las actividades que se desarrollan normalmente en el centro de procesamiento de información, que deberá incluir como mínimo el detalle de los procesos a realizar, los controles que se efectúan, los mecanismos de registración de los procesos y sus problemas, los procedimientos sobre cancelaciones y reprocesos , las relaciones con otras áreas y los mecanismos de distribución de información.

Debe constatarse la existencia de procedimientos de control para garantizar la efectivización correcta de cambios cuando corresponda, tales como: cambios de programas en bibliotecas de producción, en los archivos, cambios en las definiciones de diccionarios de datos, en las órdenes de corrida de programas , etc.

En los casos en que existan distintos centros de procesamiento debe considerar si existen responsables del control centralizado de las operaciones y procesos que se realicen en cada uno de ellos.

Debe verificar, si es necesario con pruebas, que los sistemas de información computarizados tengan incorporados en su aplicación, validaciones y controles mínimos para asegurar la integridad y validez de la información que procesan. Deben existir procedimientos de control formales que aseguren la integridad de la información que se ingresa y procesa en los sistemas.

Debe comprobar que se dispone de equipamiento alternativo (propio o por convenios formales con terceros) para el procesamiento y las telecomunicaciones, a efectos de poder superar posibles fallas o interrupciones de las actividades en sus equipos habituales. Deberá estar localizado en un edificio ubicado a una distancia razonable del centro de procesamiento.

SISTEMAS APLICATIVOS y REGISTRO DE MOVIMIENTOS.

Se debe verificar la existencia de un archivo en soporte magnético, con todas las transacciones y mensajes del sistema, para uso de los responsables del control y auditoria. Este archivo debe reunir todas las condiciones de seguridad e integridad con el fin de garantizar su confiabilidad y mantenerse disponible durante los años que fijan las normas correspondientes.

El auditor debe verificar que las operaciones que afecten a información sensible o crítica se registra, administra y procesa en los sistemas aplicativos correspondientes, no pudiendo registrarse o administrarse ninguna operación en forma manual, en planillas de cálculo u otro "software" utilitario. Debe comprobar que existan circuitos alternativos frente a posibles interrupciones del servicio.

Por cada sistema aplicativo, se deberá observar si se mantiene actualizada la documentación técnica que contenga, como mínimo: Objetivos, alcances, diagrama del sistema, registro de modificaciones, lenguaje de programación, propiedad de los programas fuentes, problemas o limitaciones conocidas, descripción del "hardware" y “software”

utilizados, descripción de las estructuras de datos, descripción de los módulos y procesos, descripción de las salidas impresas, descripción de las pantallas que permiten la modificación directa de los datos de producción (cambio de parámetros, formulas, datos, etc.) y su interrelación con las redes de telecomunicaciones.

TELEPROCESAMIENTO Y TELECOMUNICACIONES. **REDES Y ACCESOS REMOTOS**

Deberá observar si los sistemas que se utilicen para la transferencia de datos cumplen con los requisitos mínimos de controles internos establecidos en los puntos anteriores y todo lo que se refiera a la seguridad física, lógica y operación de los equipos, así como que existan circuitos alternativos frente a posibles interrupciones del servicio.

Se deberán verificar los mecanismos de protección de datos que se usan en la transmisión por la red de telecomunicaciones, si existen técnicas adecuadas de encriptación por "hardware" y/o "software".

ENCRIPTACIÓN

Se deberá insistir en la necesidad de contar, dentro de las redes de telecomunicaciones, con un "software" debidamente administrado, a fin de proveer una adecuada seguridad para los accesos a las redes, los cambios a su sistema operativo y el monitoreo de la actividad que se desarrolla en ellas.

Debe verificar que no existan usuarios con atributos similares de ingreso, verificación y/o envío de información, a fin de poder asegurar el adecuado control por oposición de intereses. Se deberán designar responsables individuales por cada uno de los atributos mencionados.

El auditor verificará las restricciones según los dominios, sus configuraciones, programas y aplicativos autorizados y los perfiles de usuarios. Debe comprobar que existan protecciones de distinto tipo, preventivas y de detección de ataques por acceso remoto o correo electrónico.

Debe describir en su informe:

- Tipo de red y conexiones
- Información transmitida, transferencia de archivos y controles existentes
- Programas y aplicaciones con acceso remoto
- Uso o no de cifrado
- Tipos de transacciones internas y externas

- Tipos de terminales
- Medidas de seguridad en las terminales y puestos de trabajo
- Como se separan Intranet e Internet, dominios, contrafuegos, proxys, etc
- Seguridad en el correo electrónico (PGP u otros controles)
- Protección de la información y de las aplicaciones
- Como se controla la página Web, intentos de accesos, modificaciones, permisos, procedimientos ante ataques.
- Si existen archivos logs de accesos realizados a otras redes, por usuario y fecha, información transferida y política de control antivirus de las transacciones.

SEGURIDAD FISICA

La seguridad es un factor de suma importancia en los centros de cómputo instalados o a instalar. Esta consideración se refleja en la elección de las normas a considerar para la ubicación del procesador, materiales utilizados para su construcción, equipo de detectores y protección contra incendios, sistema de aire acondicionado, instalación eléctrica, sistema de control de acceso y el entrenamiento al personal u operadores. El auditor deberá controlar detalladamente:

1. SITUACIÓN DEL AREA DEL CENTRO DE COMPUTOS
2. ALMACENAMIENTO DE LA INFORMACIÓN
3. EQUIPOS CONTRA INCENDIOS
4. SUMINISTRO DE ENERGIA ELECTRICA
5. SEGURIDAD EN EL ACCESO DEL PERSONAL
6. SEGURIDAD CONTRA INUNDACIONES
7. SEGURIDAD PARA EL ACCESO DE PERSONAS AL CENTRO DE CÓMPUTO
8. POLÍTICA DE BACKUPS
9. CONTROL AMBIENTAL

DERECHOS Y RESPONSABILIDAD DEL USUARIO.

El auditor deberá exigir documentos firmados por los usuarios con detalle de sus derechos, obligaciones y compromisos de uso de la red y de los puestos de trabajo y donde el GCBA se compromete a no utilizar la información privada de los agentes y ciudadanos más allá de los fines del logro de sus objetivos no admitiéndose su uso para otros propósitos ni su difusión no autorizada.

Debe verificarse que los usuarios que procesan información de personas cumplan con siguientes principios de buena práctica:

- Procesamiento de acuerdo a las leyes

- procesamiento para fines específicos
- La información que se procesa debe ser adecuada, relevante y no excesiva
- La información procesada debe ser exacta y confiable
- No guardar la información más allá de lo necesario
- La información debe ser procesada resguardando los derechos individuales
- La información procesada debe ser segura
- La información no debe ser transferida a otros organismos que no cuenten con adecuadas medidas de seguridad.

El concepto de procesamiento incluye la obtención, el mantenimiento y el revelar la información.

CONCLUSIONES:

El auditor debe orientar el objetivo de su informe en conseguir un mejoramiento de las condiciones esenciales para alcanzar el estado inicial de seguridad y de auditabilidad**.** Básicamente están implicados los siguientes ítems:

I. Definir y Documentar las políticas de seguridad de cada área.

Definir lo que hay que proteger y porque, sirve de guía para la aplicación de las medidas de protección necesarias.

II. Asignación de funciones y responsabilidades de seguridad.

El monitoreo de la seguridad en los procesos dentro de la Administración es una tarea permanente. Los cambios tecnológicos facilitan los accesos a la información y como contrapartida incrementan el riesgo. Se debe definir y establecer una adecuada misión de control según las características del área.

III. Responsabilidad del usuario en el acceso al sistema.

Cada usuario debe firmar un documento que refleje un compromiso de mantener en secreto su clave de acceso y de responsabilizarse de los cambios que se

produzcan con ella. Debe recibir esta clave de forma segura y poder administrarla a su criterio.

IV. Educación y formación en seguridad.

Todos los usuarios deben tener una capacitación general sobre los riesgos del sistema en el que están trabajando.

V. Manual de procedimientos ante incidentes de seguridad.

Debe verificar la elaboración en detalle de como se debe proceder ante los distintos incidentes detectados , como neutralizarlos e informarlo**.** Procurar una relación directa con Arcert para los casos de ataque externo.

VI. Controles físicos de la seguridad.

Debe verificar como está contemplado todo aquello que hace a factores externos que puedan interrumpir el servicio.

VII. Gestión de la seguridad en el equipamiento.

Debe verificar la existencia de seguros sobre el equipamiento.

VIII. Cumplimiento de la normativa vigente.

Debe detallar las normas y demás documentos que rigen el área.

IX. Protección, transporte y destrucción de la información.

Verificar que no se guarde la información más de lo necesario ni se manejen más datos personales que los imprescindibles para cada proceso.

Bibliografía y Organismos de Control

Este trabajo se basa en las normas y criterios de las siguientes publicaciones y organismos de control:

- COSO

  http://www.coso.org

- COBIT

  http://www.isaca.org

- Orange Book

http://www.multics.demon.uk/orange/index.htm

- British Standard 7799

  http://www.itsec.gov.uk

- MAGERIT

  http://www.map.es/csi/pg5m21.htm

- SIGEN

  http://www.sigen.gov.ar

- AGN

  http://www.agn.gov.ar

- BCRA

  http://www.bcra.gov.ar/